OGC 78-4282

30 June 1978

MEMORANDUM FOR: Deputy Director for Administration
Deputy Director for Science & Technology
Deputy Director for Operations
Deputy to the DCI for National Intelligence
Deputy to the DCI for Resource Management
Deputy to the DCI for Collection Tasking
Director, Equal Employment Opportunity
Legislative Counsel
Inspector General
Comptroller
Director of Public Affairs
Executive Secretary

STAT

FROM : [redacted]
Office of General Counsel

SUBJECT : Executive Order 12065: National Security Information

Attached for your information are an advance copy and a White House summary of the new Executive order on Government classification procedures. This Order, which replaces Executive Order 11652, becomes effective on 1 December 1978. The NSC staff also has been drafting a directive to implement the Order, and I expect it will be circulated for review within the next few weeks. If you have any questions or comments, please do not hesitate to contact me at extension [redacted]

STAT

STAT

[redacted]

Attachments

EMBARGOED UNTIL AFTER THE BRIEFING JUNE 29, 1978

Office of the White House Press Secretary

THE WHITE HOUSE

EXECUTIVE ORDER - 12065

NATIONAL SECURITY INFORMATION

By the authority vested in me as President by the Constitution and laws of the United States of America, in order to balance the public's interest in access to Government information with the need to protect certain national security information from disclosure, it is hereby ordered as follows:

TABLE OF CONTENTS

SECTION 1. ORIGINAL CLASSIFICATION.

1-1. Classification Designation.

1-101. Except as provided in the Atomic Energy Act of 1954, as amended, this Order provides the only basis for classifying information. Information may be classified

more

in one of the three designations listed below. If there is reasonable doubt which designation is appropriate, or whether the information should be classified at all, the less restrictive designation should be used, or the information should not be classified.

1-102. "Top Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

1-103. "Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

1-104. "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause identifiable damage to the national security.

1-2. Classification Authority.

1-201. Top Secret. Authority for original classification of information as Top Secret may be exercised only by the President, by such officials as the President may designate by publication in the Federal Register, by the agency heads listed below, and by officials to whom such authority is delegated in accordance with Section 1-204:

The Secretary of State
The Secretary of the Treasury
The Secretary of Defense
The Secretary of the Army
The Secretary of the Navy
The Secretary of the Air Force
The Attorney General
The Secretary of Energy
The Chairman, Nuclear Regulatory Commission
The Director, Arms Control and Disarmament Agency
The Director of Central Intelligence
The Administrator, National Aeronautics and Space Administration
The Administrator of General Services (delegable only to the Director, Federal Preparedness Agency and to the Director, Information Security Oversight Office)

1-202. Secret. Authority for original classification of information as Secret may be exercised only by such officials as the President may designate by publication in the Federal Register, by the agency heads listed below, by officials who have Top Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204:

The Secretary of Commerce
The Secretary of Transportation
The Administrator, Agency for International Development
The Director, International Communication Agency

1-203. Confidential. Authority for original classification of information as Confidential may be exercised only by such officials as the President may designate by publication in the Federal Register, by the agency heads listed below, by officials who have Top Secret or Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204:

The President and Chairman, Export-Import Bank of the United States
The President and Chief Executive Officer, Overseas Private Investment Corporation

1-204. Limitations on Delegation of Classification Authority.

(a) Authority for original classification of information as Top Secret may be delegated only to principal subordinate officials who have a frequent need to exercise such authority as determined by the President or by agency heads listed in Section 1-201.

(b) Authority for original classification of information as Secret may be delegated only to subordinate officials who have a frequent need to exercise such authority as determined by the President, by agency heads listed in Sections 1-201 and 1-202, and by officials with Top Secret classification authority.

(c) Authority for original classification of information as Confidential may be delegated only to subordinate officials who have a frequent need to exercise such authority as determined by the President, by agency heads listed in Sections 1-201, 1-202, and 1-203, and by officials with Top Secret classification authority.

(d) Delegated original classification authority may not be redelegated.

(e) Each delegation of original classification authority shall be in writing (by name or title of position held.)

(f) Delegations of original classification authority shall be held to an absolute minimum. Periodic reviews of such delegations shall be made to ensure that the officials so designated have demonstrated a continuing need to exercise such authority.

1-205. Exceptional Cases. When an employee or contractor of an agency that does not have original classification authority originates information believed to require classification, the information shall be protected in the manner prescribed by this Order and implementing directives. The information shall be transmitted promptly under appropriate safeguards to the agency which has appropriate subject matter interest and classification authority. That agency shall decide within 30 days whether to classify that information. If it is not clear which agency should get the information, it shall be sent to the Director of the Information Security Oversight Office established in Section 5-2 for a determination.

1-3. Classification Requirements.

1-301. Information may not be considered for classification unless it concerns:

(a) military plans, weapons, or operations;

(b) foreign government information;

(c) intelligence activities, sources or methods;

(d) foreign relations or foreign activities of the United States;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities; or

more

(OVER)

(g) other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the President, by a person designated by the President pursuant to Section 1-201, or by an agency head.

1-302. Even though information is determined to concern one or more of the criteria in Section 1-301, it may not be classified unless an original classification authority also determines that its unauthorized disclosure reasonably could be expected to cause at least identifiable damage to the national security.

1-303. Unauthorized disclosure of foreign government information or the identity of a confidential foreign source is presumed to cause at least identifiable damage to the national security.

1-304. Each determination under the criterion of Section 1-301(g) shall be reported promptly to the Director of the Information Security Oversight Office.

1-4. Duration of Classification.

1-401. Except as permitted in Section 1-402, at the time of the original classification each original classification authority shall set a date or event for automatic declassification no more than six years later.

1-402. Only officials with Top Secret classification authority and agency heads listed in Section 1-2 may classify information for more than six years from the date of the original classification. This authority shall be used sparingly. In such cases, a declassification date or event, or a date for review, shall be set. This date or event shall be as early as national security permits and shall be no more than twenty years after original classification, except that for foreign government information the date or event may be up to thirty years after original classification.

1-5. Identification and Markings.

1-501. At the time of original classification, the following shall be shown on the face of paper copies of all classified documents:

(a) the identity of the original classification authority;

(b) the office of origin;

(c) the date or event for declassification or review; and

(d) one of the three classification designations defined in Section 1-1.

1-502. Documents classified for more than six years shall also be marked with the identity of the official who authorized the prolonged classification. Such documents shall be annotated with the reason the classification is expected to remain necessary, under the requirements of Section 1-3, despite the passage of time. The reason for the prolonged classification may be stated by reference to criteria set forth in agency implementing regulations. These criteria shall explain in narrative form the reason the information needs to be protected beyond six years. If the individual who signs or otherwise authenticates a document also is authorized to classify it, no further annotation of identity is required.

more

1-503. Only the designations prescribed by this Order may be used to identify classified information. Markings such as "For Official Use Only" and "Limited Official Use" may not be used for that purpose. Terms such as "Conference" or "Agency" may not be used in conjunction with the classification designations prescribed by this Order; e.g., "Agency Confidential" or "Conference Confidential."

1-504. In order to facilitate excerpting and other uses, each classified document shall, by marking or other means, indicate clearly which portions are classified, with the applicable classification designation, and which portions are not classified. The Director of the Information Security Oversight Office may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information.

1-505. Foreign government information shall either retain its original classification designation or be assigned a United States classification designation that shall ensure a degree of protection equivalent to that required by the entity that furnished the information.

1-506. Classified documents that contain or reveal information that is subject to special dissemination and reproduction limitations authorized by this Order shall be marked clearly so as to place the user on notice of the restrictions.

1-6. Prohibitions.

1-601. Classification may not be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition.

1-602. Basic scientific research information not clearly related to the national security may not be classified.

1-603. A product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified under this Order until and unless the government acquires a proprietary interest in the product. This Order does not affect the provisions of the Patent Secrecy Act of 1952 (35 U.S.C. 181-188).

1-604. References to classified documents that do not disclose classified information may not be classified or used as a basis for classification.

1-605. Classification may not be used to limit dissemination of information that is not classifiable under the provisions of this Order or to prevent or delay the public release of such information.

1-606. No document originated on or after the effective date of this Order may be classified after an agency has received a request for the document under the Freedom of Information Act or the Mandatory Review provisions of this Order (Section 3-5), unless such classification is consistent with this Order and is authorized by the agency head (or deputy agency head). Documents originated before the effective date of this Order and subject to such a request may not be classified unless such classification is consistent with this Order and is authorized by the senior official designated to oversee the agency information security program or by an official with Top Secret classification authority. Classification authority under this provision shall be exercised personally, on a document-by-document basis.

more

(OVER)

1-607. Classification may not be restored to documents already declassified and released to the public under this Order or prior Orders.

SECTION 2. DERIVATIVE CLASSIFICATION.

2-1. Use of Derivative Classification.

2-101. Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide.

2-102. Persons who apply such derivative classification markings shall:

(a) respect original classification decisions;

(b) verify the information's current level of classification so far as practicable before applying the markings; and

(c) carry forward to any newly created documents the assigned dates or events for declassification or review and any additional authorized markings, in accordance with Sections 2-2 and 2-301 below. A single marking may be used for documents based on multiple sources.

2-2. Classification Guides.

2-201. Classification guides used to direct derivative classification shall specifically identify the information to be classified. Each classification guide shall specifically indicate how the designations, time limits, markings, and other requirements of this Order are to be applied to the information.

2-202. Each such guide shall be approved personally and in writing by an agency head listed in Section 1-2 or by an official with Top Secret classification authority. Such approval constitutes an original classification decision.

2-3. New Material.

2-301. New material that derives its classification from information classified on or after the effective date of this Order shall be marked with the declassification date or event, or the date for review, assigned to the source information.

2-302. New material that derives its classification from information classified under prior Orders shall be treated as follows:

(a) If the source material bears a declassification date or event twenty years or less from the date of origin, that date or event shall be carried forward on the new material.

(b) If the source material bears no declassification date or event or is marked for declassification beyond twenty years, the new material shall be marked with a date for review for declassification at twenty years from the date of original classification of the source material.

(c) If the source material is foreign government information bearing no date or event for declassification or is marked for declassification beyond thirty years, the

more

new material shall be marked for review for declassification at thirty years from the date of original classification of the source material.

SECTION 3. DECLASSIFICATION AND DOWNGRADING.

3-1. Declassification Authority.

3-101. The authority to declassify or downgrade information classified under this or prior Orders shall be exercised only as specified in Section 3-1.

3-102. Classified information may be declassified or downgraded by the official who authorized the original classification if that official is still serving in the same position, by a successor, or by a supervisory official of either.

3-103. Agency heads named in Section 1-2 shall designate additional officials at the lowest practicable echelons to exercise declassification and downgrading authority.

3-104. If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified until the appeal is decided or until one year from the date of the Director's decision, whichever occurs first.

3-105. The provisions of this Order relating to declassification shall also apply to agencies which, under the terms of this Order, do not have original classification authority but which had such authority under prior Orders.

3-2. Transferred Information.

3-201. For classified information transferred in conjunction with a transfer of functions -- not merely for storage purposes -- the receiving agency shall be deemed to be the originating agency for all purposes under this Order.

3-202. For classified information not transferred in accordance with Section 3-201, but originated in an agency which has ceased to exist, each agency in possession shall be deemed to be the originating agency for all purposes under this Order. Such information may be declassified or downgraded by the agency in possession after consulting with any other agency having an interest in the subject matter.

3-203. Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and the agency guidelines.

more

(OVER)

3-204. After the termination of a Presidential administration, the Archivist of the United States (shall) review ( ) and declassify or downgrade all information classified by the President, the White House Staff, committees or commissions appointed by the President, or others acting on the President's behalf. (Such declassification shall only be undertaken in accordance with the provisions of Section 3-504.) (... authority shall be exercised only after consultation with the agencies having primary subject matter interest; Any decision of the Archivist may be appealed ... order of ...) | ← A

3-3. Declassification Policy.

3-301. Declassification of classified information shall be given emphasis comparable to that accorded classification. Information classified pursuant to this and prior Orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or on the occurrence of a declassification event.) ( )

3-302. When information is reviewed for declassification (pursuant to this Order or the Freedom of Information Act), it shall be declassified unless the declassification authority established pursuant to Section 3-1 determines that the information continues to meet the classification requirements prescribed in Section 1-3 despite the passage of time.

( )
3-303. It is presumed that information which continues to meet the (classification requirements) in Section 1-3 requires continued protection. In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head, a senior agency official with responsibility for processing Freedom of Information Act requests (or) Mandatory Review requests under this Order, an official with Top Secret classification authority, or the Archivist of the United States in the case of material covered in Section 3-503. That official will determine whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

3-4. Systematic Review for Declassification.

3-401. Classified information constituting permanently valuable records of the Government, as defined by 44 U.S.C. 2103, and information in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be reviewed for declassification as it becomes twenty years old. Agency heads listed in Section 1-2 and officials designated by the President pursuant to Section 1-201 of this Order may extend classification beyond twenty years, but only in accordance with Sections 3-3 and 3-402. This authority may not be delegated. When classification is extended beyond twenty years, a date no more than ten years later shall be set for declassification or for the next review. That date shall be marked on the document. Subsequent reviews for declassification shall be set at no more than ten year intervals. The Director of the Information Security Oversight Office may extend the period between subsequent reviews for specific categories of documents or information.

more

A ... This now requires consultation only with an originating agency, rather than with an agency having primary interest ... ...)

3-402. Within 180 days after the effective date of this Order, the agency heads listed in Section 1-2 and the heads of agencies which had original classification authority under prior orders shall, after consultation with the Archivist of the United States and review by the Information Security Oversight Office, issue and maintain guidelines for systematic review covering twenty-year old classified information under their jurisdiction. These guidelines shall state specific, limited categories of information which, because of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond twenty years is needed. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information. All information not identified in these guidelines as requiring review and for which a prior automatic declassification date has not been established shall be declassified automatically at the end of twenty years from the date of original classification.

3-403. Notwithstanding Sections 3-401 and 3-402, the Secretary of Defense may establish special procedures for systematic review and declassification of classified cryptologic information, (and the Director of Central Intelligence may establish special procedures for systematic review and declassification of classified information concerning the identities of clandestine human agents). These procedures shall be consistent, so far as practicable, with the objectives of Sections 3-401 and 3-402. Prior to implementation, they shall be reviewed and approved by the Director of the Information Security Oversight Office and, with respect to matters pertaining to intelligence sources and methods, by the Director of Central Intelligence. (Disapproval of procedures) by the Director of the Information Security Oversight Office may be appealed to the National Security Council. In such cases, the procedures shall not be implemented until the appeal is decided.

3-404. Foreign government information shall be exempt from automatic declassification and twenty year systematic review. Unless declassified earlier, such information shall be reviewed for declassification thirty years from its date of origin. Such review shall be in accordance with the provisions of Section 3-3 and with guidelines developed by agency heads in consultation with the Archivist of the United States and, where appropriate, with the foreign government or international organization concerned. (These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information.)

3-405. Transition to systematic review at twenty years shall be implemented as rapidly as practicable and shall be completed no more than ten years from the effective date of this Order.

3.5 Mandatory Review for Declassification.

3-501. (Agencies shall establish a mandatory review procedure) to handle requests by a member of the public, by a government employee, or by an agency, to declassify and release information. (This procedure) shall apply to information classified under this Order or prior Orders. Except as provided in Section 3-503, upon such a request the information shall be reviewed for possible declassification, provided the request (reasonably describes the information.)

more

(OVER)

Requests for declassification under this provision shall be acted upon within 60 days. (After review, the information or any reasonably segregable portion thereof that no longer requires protection under this Order shall be declassified and released unless withholding is otherwise warranted under applicable law.)

3-502. Requests for declassification which are submitted under the provisions of the Freedom of Information Act shall be processed in accordance with the provisions of that Act.

3-503. Information less than ten years old which was originated by the President, by the White House Staff, or by committees or commissions appointed by the President, or by others acting on behalf of the President, including such information in the possession and control of the Administrator of General Services pursuant to 44 U.S.C. 2107 or 2107 note, is exempted from the provisions of Section 3-501. Such information over ten years old shall be subject to mandatory review for declassification. Requests for mandatory review shall be processed in accordance with procedures developed by the Archivist of the United States. These procedures shall provide for consultation with agencies having primary subject matter interest. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council through the process set forth in Section 3-104.

3-504. Requests for declassification of classified documents originated by an agency but in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be referred by the Archivist to the agency of origin for processing in accordance with Section 3-501 and for direct response to the requestor. The Archivist shall inform requestors of such referrals.

3-505. No agency in possession of a classified document may, in response to a request for the document made under the Freedom of Information Act or this Order's Mandatory Review provision, refuse to confirm the existence or non-existence of the document, unless the fact of its existence or non-existence would itself be classifiable under this Order.

3-6. Downgrading.

3-601. Classified information that is marked for automatic downgrading is downgraded accordingly without notification to holders.

3-602. Classified information that is not marked for automatic downgrading may be assigned a lower classification designation by the originator or by other authorized officials when such downgrading is appropriate. Notice of downgrading shall be provided to holders of the information to the extent practicable.

SECTION 4. SAFEGUARDING.

4-1. General Restrictions on Access.

4-101. No person may be given access to classified information unless that person has been determined to be trustworthy and unless access is necessary for the performance of official duties.

more

4-102. All classified information shall be marked conspicuously to put users on notice of its current classification status and, if appropriate, to show any special distribution or reproduction restrictions authorized by this Order.

4-103. Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, and transmitted only under conditions that will provide adequate protection and prevent access by unauthorized persons.

4-104. Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of Chapters 21 and 33 of Title 44 of the United States Code, which governs disposition of Federal records.

4-105. Classified information disseminated outside the Executive branch shall be given protection equivalent to that afforded within the Executive branch.

4-2. Special Access Programs.

4-201. Agency heads listed in Section 1-201 may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or prior Orders. Such programs may be created or continued only by written direction and only by those agency heads and, for matters pertaining to intelligence sources and methods, by the Director of Central Intelligence. Classified information in such programs shall be declassified according to the provisions of Section 3.

4-202. Special access programs may be created or continued only on a specific showing that:

(a) normal management and safeguarding procedures are not sufficient to limit need-to-know or access;

(b) the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved; and

(c) the special access controls balance the need to protect the information against the full spectrum of needs to use the information.

4-203. All special access programs shall be reviewed regularly and, except those required by treaty or international agreement, shall terminate automatically every five years unless renewed in accordance with the procedures in Section 4-2.

4-204. Within 180 days after the effective date of this Order, agency heads shall review all existing special access programs under their jurisdiction and continue them only in accordance with the procedures in Section 4-2. Each of those agency heads shall also establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office shall have non-delegable access to all such accountings.

more

(OVER)

4-3. Access by Historical Researchers and Former Presidential Appointees.

4-301. The requirement in Section 4-101 that access to classified information may be granted only as is necessary for the performance of official duties may be waived as provided in Section 4-302 for persons who:

(a) are engaged in historical research projects, or

(b) previously have occupied policy-making positions to which they were appointed by the President.

4-302. Waivers under Section 4-301 may be granted only if the agency with jurisdiction over the information:

(a) makes a written determination that access is consistent with the interests of national security;

(b) takes (appropriate steps) to ensure that access is limited to specific categories of information over which that agency has classification jurisdiction;

(c) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed or received while serving as a Presidential appointee.

4-4. Reproduction Controls.

4-401. Top Secret documents may not be reproduced without the consent of the originating agency unless otherwise marked by the originating office.

4-402. Reproduction of Secret and Confidential documents may be restricted by the originating agency.

4-403. Reproduced copies of classified documents are subject to the same accountability and controls as the original documents.

4-404. Records shall be maintained by all agencies that reproduce paper copies of classified documents to show the number and distribution of reproduced copies of all Top Secret documents, of all documents covered by special access programs distributed outside the originating agency, and of all Secret and all Confidential documents which are marked with special dissemination and reproduction limitations in accordance with Section 1-506.

4-405. Sections 4-401 and 4-402 shall not restrict the reproduction of documents for the purpose of facilitating review for declassification. However, such reproduced documents that remain classified after review must be destroyed after they are used.

SECTION 5. IMPLEMENTATION AND REVIEW.

5-1. Oversight.

5-101. The National Security Council may review all matters with respect to the implementation of this Order and shall provide overall policy direction for the information security program.

more

5-102. The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. This responsibility shall be delegated to an Information Security Oversight Office.

5-2. Information Security Oversight Office.

5-201. The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Administrator also shall have authority to appoint a staff for the Office.

5-202. The Director shall:

(a) oversee agency actions to ensure compliance with this Order and implementing directives;

(b) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program, including appeals from decisions on declassification requests pursuant to Section 3-503;

(c) exercise the authority to declassify information provided by Sections 3-104 and 3-503;

(d) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order which shall be binding on the agencies;

(e) report annually to the President through the Administrator of General Services and the National Security Council on the implementation of this Order;

(f) review all agency implementing regulations and guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect until the appeal is decided or until one year from the date of the Director's decision, whichever occurs first.

(g) exercise case-by-case classification authority in accordance with Section 1-205 and review requests for original classification authority from agencies or officials not granted original classification authority under Section 1-2 of this Order; and

(h) have the authority to conduct on-site reviews of the information security program of each agency that handles classified information and to require of each agency such reports, information, and other cooperation as necessary to fulfill his responsibilities. If such reports, inspection, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect until the appeal is decided or until one year from the date of the denial, whichever occurs first.

more

(OVER)

5-3. Interagency Information Security Committee.

5-301. There is established an Interagency Information Security Committee which shall be chaired by the Director and shall be comprised of representatives of the Secretaries of State, Defense, Treasury, and Energy, the Attorney General, the Director of Central Intelligence, the National Security Council, the Domestic Policy Staff, and the Archivist of the United States.

5-302. Representatives of other agencies may be invited to meet with the Committee on matters of particular interest to those agencies.

5-303. The Committee shall meet at the call of the Chairman or at the request of a member agency and shall advise the Chairman on implementation of this Order.

5-4. General Responsibilities.

5-401. A copy of any (information security) regulation and a copy of any guideline for systematic (declassification) review which has been adopted pursuant to this Order or implementing directives, shall be submitted to the Information Security Oversight Office. To the extent practicable, such regulations and guidelines should be unclassified.

5-402. Unclassified regulations that establish agency information security policy (and unclassified guidelines for systematic declassification review) shall be published in the Federal Register.

5-403. Agencies with original classification authority shall promulgate guides for security classification that will facilitate the identification and uniform classification of information requiring protection under the provisions of this Order.

5-404. Agencies which originate or handle classified information shall:

(a) designate a senior agency official to conduct an active oversight program to ensure effective implementation of this Order;

(b) designate a senior agency official to chair an agency committee with authority to act on all suggestions and complaints with respect to the agency's administration of the information security program;

(c) establish a process to decide appeals from denials of declassification requests submitted pursuant to Section 3-5;

(d) establish a program to familiarize agency and other personnel who have access to classified information with the provisions of this Order and implementing directives. This program shall impress upon agency personnel their responsibility to exercise vigilance in complying with this Order. The program shall encourage agency personnel to challenge, through Mandatory Review and other appropriate procedures, those classification decisions (they) believe to be improper;

(e) promulgate guidelines for systematic review in accordance with Section 3-402;

more

(f) establish procedures to prevent unnecessary access to classified information, including procedures which require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and which ensures that the number of people granted access to classified information is reduced to and maintained at the minimum number that is consistent with operational requirements and needs; and

(g) ensure that practices for safeguarding information are systematically reviewed and that those which are duplicative or unnecessary are eliminated.

5-405. Agencies shall submit to the Information Security Oversight Office such information or reports as the Director of the Office may find necessary to carry out the Office's responsibilities.

5-5. Administrative Sanctions.

5-501. If the Information Security Oversight Office finds that a violation of this Order or any implementing directives may have occurred, it shall make a report to the head of the agency concerned so that corrective steps may be taken.

5-502. Officers and employees of the United States Government shall be subject to appropriate administrative sanctions if they:

(a) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directives; or

(b) knowingly, willfully and without authorization disclose information properly classified under this Order or prior Orders or compromise properly classified information through negligence; or

(c) knowingly and willfully violate any other provision of this Order or implementing directive.

5-503. Sanctions may include reprimand, suspension wihout pay, removal, termination of classification authority, or other sanction in accordance with applicable law and agency regulations.

5-504. Agency heads shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5-502 occurs. The Director of the Information Security Oversight Office shall be informed when such violations occur.

5-505. Agency heads shall report to the Attorney General evidence reflected in classified information of possible violations of Federal criminal law by an agency employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General.

SECTION 6. GENERAL PROVISIONS

6-1. Definitions.

6-101. "Agency" has the meaning defined in 5 U.S.C. 552(e).

more

(OVER)

6-102. "Classified information" means information or material, herein collectively termed information, that is owned by, produced for or by, or under the control of, the United States Government, and that has been determined pursuant to this Order (or prior Orders) to require protection against unauthorized disclosure, and that is so designated.

6-103. "Foreign government information" means information that has been provided to the United States in confidence by, or produced by the United States pursuant to a written joint arrangement requiring confidentiality with, a foreign government or international organization of governments.

6-104. "National security" means the national defense and foreign relations of the United States.

6-105. "Declassification event" means an event which would eliminate the need for continued classification.

6-2. General.

6-201. Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and information designated as "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued pursuant thereto.

6-202. The Attorney General, upon request by the head of an agency, his duly designated representative, or the Director of the Information Security Oversight Office, shall personally or through authorized representatives of the Department of Justice render an interpretation of this Order with respect to any question arising in the course of its administration.

6-203. Executive Order No. 11652 of March 8, 1972, as amended by Executive Order No. 11714 of April 24, 1973, and (as further amended by Executive Order) No. 11862 of June 11, 1975, and the National Security Council Directive of May 17, 1972 (3 C.F.R. 1085 (1971-75 Comp.)) are revoked.

6-204. This Order shall become effective on December 1, 1978, except that the functions of the Information Security Oversight Office specified in Sections 5-202(d) and 5-202(f) shall be effective immediately and shall be performed in the interim by the Interagency Classification Review Committee established pursuant to Executive Order No. 11652.

JIMMY CARTER

THE WHITE HOUSE,
June 28, 1978.

# # # #

EMBARGOED FOR RELEASE
AFTER THE BRIEFING

JUNE 29, 1978

Office of the White House Press Secretary

THE WHITE HOUSE

Fact Sheet: The new Executive Order on the Security Classification System

The new Executive Order was drafted by an interagency study team led by the National Security Council and Domestic Policy staffs. The study included consultation with interested Congressional committees and public interest groups. The new Order replaces Executive Order 11652, which was issued in 1972.

The major changes from Executive Order 11652 are as follows:

(1) Under the old system, a document could be classified if its unauthorized disclosure could reasonably be expected to damage national security. Under the new Order, two tests must be met:

-- the information must fall within one of seven classification criteria; and

-- the damage must be identifiable.

The word "identifiable" has been added to tighten the standard -- to prevent classification when the damage would be insignificant. That change and the addition of the criteria are intended to make classifiers' decisions more thoughtful and less automatic.

Six of the criteria outline the subject areas for classification, such as intelligence sources and the design of weapons. The seventh allows agency heads to designate additional, narrow national security areas that may have been omitted by the first six. This authority will be used rarely, and each use must be reported to the oversight office created by the Order.

(2) The new Order requires that most documents be classified section-by-section, not as a whole.

The Order retains the three-level classification system. (Top Secret for documents the disclosure of which would cause exceptionally grave damage to the national security; Secret for serious damage; and Confidential for identifiable damage.) Under the old system, most documents were marked with the highest classification level of any portion. As a result, much information was unnecessarily classified, since a document of dozens of pages might have only a few paragraphs that require classification, but the entire document would be classified. This problem was compounded by the fact that most classification is "derivative" -- i.e. based on references to other classified documents. Under the old system, a new document that referred to any portion of a classified document would have to be given the same classification because there was no way to tell whether the portion was classified.

The new procedure will allow ready identification of the classification level -- if any -- of each section of a document. This will avert unnecessary and overly high classification of many documents.

more

This requirement will be waived for a few categories of documents where it is unworkable (e.g., computer-generated items.)

(3) Classification of privately owned documents is forbidden unless the government acquires a proprietary interest in them or its creator used classified information, except as otherwise provided by statute.

(4) Eleven agencies are stripped of classification authority:

(1) Department of Health, Education, and Welfare
(2) Department of Agriculture
(3) Department of Labor
(4) Federal Energy Regulatory Commission
(5) Interstate Commerce Commission
(6) Federal Communications Commission
(7) Civil Service Commission
(8) Civil Aeronautics Board
(9) National Science Foundation
(10) Federal Maritime Commission
(11) Domestic Policy Staff (formerly Domestic Council)

Five other agencies get reduced authority:

(1) Department of Commerce (Top Secret to Secret)
(2) Agency for International Development (Top Secret to Secret)
(3) Overseas Private Investment Corporation (Secret to Confidential)
(4) Export-Import Bank (Secret to Confidential)
(5) Council of Economic Advisers (Top Secret to Secret)

No agency is given increased classification authority. (These changes apply to original classfication authority -- not derivative classification.)

(5) The new Order restricts the number of officials to whom classification authority may be delegated and forbids redelegation. These changes are unlikely to reduce the number with Top Secret authority (only 1,400 out of over six million Federal civilian and military employees), but there should be some reduction in the number with Secret and Confidential authority (a total of 11,900).

(6) The new Order restricts the use of classification after a document has been requested under the Freedom of Information Act (FOIA) or the non-statutory "Mandatory Review" procedure. In theory, all documents should be classified when they are written but errors are sometimes made, and agencies need to be able to classify documents late. At present, there are no restrictions on classification after an FOIA request. Under the new Order, only senior agency officials can classify existing documents in such circumstances. For documents originated after the Order goes into effect, the authority is further limited to the agency head and the deputy.

Duration of Classification

(7) The duration of classification is cut sharply.

Under the old system, an estimated 47% of the documents classified each year were covered by the General Declassification Schedule (GDS). These documents were

more

automatically declassified after six to ten years, depending on whether they were Confidential, Secret, or Top Secret. The other 53% were exempted from GDS by officials with Top Secret classification authority. (In theory, such exemptions were limited to four categories, but the categories were drawn so broadly they were ineffective, and they were often disregarded altogether.) Most documents exempted from GDS stayed classified until they were 30 years old. At that point, they would be reviewed and declassified, except for a few items for which agency heads would extend classification indefinitely.

The new system abolishes GDS and makes the duration of classification depend on the content of the information, not its classification level. Most documents will be automatically declassified after six years or less. Agency heads and officials with Top Secret authority may set longer terms, but the Order requires them to state why the document will continue to meet the test for classification despite the passage of time. Documents given longer terms will now be reviewed and declassified when they are 20 years old instead of 30. As in the old system, agency heads will extend classification for a few items, but the new Order requires additional review every ten years. (The new Order also permits extended classification for cryptographic materials; that is the practice at present.)

The new Order makes declassification of old documents faster and less expensive. It requires agencies to cooperate with the National Archives in drafting guidelines which will let the Archives review and declassify most documents on its own, without having to forward them to the agency to review.

The National Archives estimates that the change from 30 to 20 years will result in declassification of an extra 250 million pages over the next decade. (Without the change, about 350 million pages would have been released in that period.) The shift from GDS to six years will mean faster declassification for millions more documents when the first items classified under this Order become six years old.

Declassification Process

(8) The new Order makes it clear that a request for release of a document cannot be rejected merely because the document is classified. The agency must examine the document to see whether its release would still do identifiable damage to the national security in spite of the passage of time. It it would not, the document will be declassified.

(9) For the first time, the declassification process will include a "balancing test." In appropriate cases the public's interest in knowing the information is to be balanced against the need to keep it secret. When the interest in disclosure is greater, the information will be released even though its continued classification is justified.

(10) Agencies are required to declassify information as early as national security permits and to give declassification as high a priority as classification. In addition, the number of officials authorized to declassify will be increased.

more

(OVER)

Other Changes

(11) An Information Security Oversight Office is created to police the classification system. (At present, there is an interagency committee which has limited authority.) The new Office will be located in the General Services Administration under the supervision of the National Security Council.

(12) At present, there are hundreds of "special access" programs (also called "compartments") which restrict access to highly sensitive classified information. These programs are expensive to maintain and may prevent or delay access by policy officials who really need the information. In addition, the proliferation of these programs has reduced their protection value.

The new Order allows agencies to continue such programs -- they are needed in special cases -- but it will reduce their number. Henceforth, these programs may be continued or created only upon a written finding of necessity by an agency head. A "sunset" provision will terminate each program after five years unless a new determination of need is made.

(13) Agencies are required to impose administrative penalties for unnecessary or excessive classification and for disclosure or compromise of properly classified information. The new Order also creates procedures to assure that violations of law are reported to the Justice Department.

(14) The new Order tightens administrative restrictions on copying and dissemination of classified documents, including a requirement that records be kept of all copies Top Secret documents and certain others.

(15) Special treatment is provided for national security information obtained in confidence from foreign governments or international organizations. Such information will be presumed to meet the test for classification and may be classified for up to 30 years instead of 20. All the other requirements of the new Order apply, however. This provision was added because most allied governments are more restrictive than the U.S., and without such special treatment they might stop supplying us with valuable information.

(16) The use of classification to conceal violations of law is forbidden.

(17) The new Order says that classification may not be restored to documents once they are officially released to the public.

(18) The new Order forbids the use of classification to limit dissemination of information that does not merit classification or to prevent or delay the public release of such information.

(19) Agencies are required to establish classification guides to promote uniformity in classification level and duration.

# # # # #